IN THE COURT OF APPEALS OF THE
STATE OF OREGON

STATE OF OREGON,
Plaintiff-Respondent,
v.
NATHAN COMBEST,
Defendant-Appellant.

Lane County Circuit Court
201203470; A151950

Mustafa T. Kasubhai, Judge.

Argued and submitted August 19, 2014.

Mary M. Reese, Senior Deputy Public Defender, argued the cause for appellant. With her on the brief was Peter Gartlan, Chief Defender, Office of Public Defense Services.

Michael J. Slauson, Senior Assistant Attorney General, argued the cause for respondent. With him on the brief were Ellen F. Rosenblum, Attorney General, and Anna M. Joyce, Solicitor General.

Before Sercombe, Presiding Judge, and Hadlock, Judge, and Tookey, Judge.

SERCOMBE, P. J.

Affirmed.

SERCOMBE, P. J.

Defendant appeals a judgment of conviction for multiple counts of encouraging child sexual abuse, assigning error to the trial court's denial of his motion to suppress evidence. Defendant shared files, including files containing child pornography, on a peer-to-peer computer network. Using software called Shareaza LE, officers accessed that peer-to-peer network; searched for shared files that, in light of file name and other attributes, were likely child pornography; identified an IP address for a user sharing those files; and then downloaded two files from that user. They later identified defendant as that user and uncovered other evidence from defendant's computer that he possessed child pornography. On appeal, defendant argues, as he did in the trial court, that all evidence of his distribution and possession of child pornography should be suppressed because the officers conducted a warrantless "search" under Article I, section 9, of the Oregon Constitution[1]—*i.e.*, they invaded defendant's protected privacy interest—when they used Shareaza LE to locate and access his files on the peer-to-peer network. As detailed below, we conclude that, because the officers used Shareaza LE to access selective information that defendant made available to any other user of the peer-to-peer network by targeting shared network files containing child pornography, their use of that software did not amount to a search under Article I, section 9. Accordingly, we affirm.

We review the trial court's denial of defendant's motion to suppress for legal error, and we describe the facts consistently with the trial court's explicit and implicit findings, which the evidence supports. *State v. Ehly*, 317 Or 66, 75, 854 P2d 421 (1993). We start by detailing the operation of Shareaza LE, as explained by a detective and a forensics analyst from the Lane County Sheriff's Office, before describing how they used that software in this case.

Peer-to-peer file sharing permits a computer user to share files with other users on a particular peer-to-peer

[1] Article I, section 9, provides that "[n]o law shall violate the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search, or seizure[.]"

network. To access the peer-to-peer network that defendant used in this case, eDonkey, a user must download client application software. Defendant used software called eMule. That software allows a user to search all the files that other online network users are sharing by entering search terms. A user is online if he has logged into eMule and has it running on his computer; the number of users running eMule at any given time ranges from several hundred thousand to many million.

After a user enters search terms, eMule creates a list of results, and a user can then click on a file to download. When downloading a file, eMule puts the file immediately into a "Temp" folder; when a file is completely downloaded, eMule moves the file to an "Incoming" folder. The eMule software automatically creates those folders, and the files in those folders are automatically shared with other users on the network. A user can prevent other users from gaining access to a downloaded file by moving that file out of the Temp or Incoming folders on the user's computer. But downloaded files that remain in those folders are available for download by other users.

The peer-to-peer network, eDonkey, "hashes" the files on the network; that is, it uses a complex mathematical algorithm to generate an alphanumeric identifier—a hash value—unique to each file. One of the officers in this case described a hash value as "more accurate than DNA."[2] He testified that, if a user downloaded a digital picture and "remove[d] one pixel out of that, the whole hash value changes." But if a user changes the file name without changing the file itself, the hash value stays the same. Two files that are exactly the same (even if they have different file names) will have the same hash value.

Hash values are therefore useful to police officers who monitor peer-to-peer networks for the exchange of

[2] A hash value has also been described as "a kind of 'digital fingerprint.'" *U.S. v. Wellman*, 663 F3d 224, 226 n 2 (4th Cir 2011) (noting that the district court found that files with the same hash value have a 99.99 percent probability of being identical). The upshot is that it is highly improbable that two files with the same hash value will have different content.

child pornography.[3] The National Center for Missing and Exploited Children (NCMEC) keeps a list of the hash values of shared files—pictures and videos—that are known to contain child pornography. One way for law enforcement to quickly identify files that contain child pornography, then, is to look for hash values that match those on the NCMEC list, because hash values stay constant as the same file is copied and exchanged, even if the file name is changed.

In this case, the Lane County Sheriff's Office used software called Shareaza LE to find files on the eDonkey network that it suspected contain child pornography. Shareaza LE performs an automated search for child pornography by automatically ticking through and entering a rotating list of search terms commonly used to obtain child pornography. For the files that match those search terms, Shareaza LE goes through a "vetting" process and targets those files that have a hash value identified by the NCMEC as "child notable."

Shareaza LE narrows its search to a particular jurisdiction. It does this by identifying the Internet Protocol (IP) address associated with users on the network and narrowing its search to a particular set of IP addresses. An IP address is a unique number assigned by an Internet Service Provider (ISP) like Comcast or Charter Cable to a customer's modem, and police can generally track particular IP addresses to a particular geographic region.[4] Assuming that a customer has only one ISP, the customer has one IP address, no matter how many devices are connected to the Internet using that service. Because Shareaza LE can narrow its search to IP addresses in a particular region, officers

[3] Hash values also enable faster downloads for eMule users. Even if users give the same file a different file name, eMule can identify duplicate files by their hash values. As a result, when a user selects a file to download, eMule can create a new file for the user by copying pieces of it from various users on the network (a faster method than downloading the entire file from one other user). eMule then puts those pieces together and compares the hash value of the newly created file with the source files to ensure that the new file is complete.

[4] One of the officers explained that "the IP addresses are assigned by the Internet Service Providers and they have communications equipment in various places. At the major hubs, those communication equipments also contain the latitude [and] longitude of the location where that equipment is. That's how [Shareaza LE] determines initially that that IP address may be in that jurisdiction."

do not have to "search thousands and thousands" of files to find one with an IP address in their jurisdiction.

Besides the IP address, Shareaza LE identifies the Globally Unique Identifier (GUID) given to a specific computer on the peer-to-peer network. In contrast to an IP address, the GUID is specific to a particular user's eMule software installed on a particular computer. Because the probability of two eMule software applications having the same GUID is extremely small, officers can confidently match the GUID from a downloaded file containing child pornography with the GUID of particular eMule software on a computer.

Once an officer finds a specific file with a particular IP address to download, the officer uses Shareaza LE to download that file from the user at that IP address. In that respect, Shareaza LE is different than other software, like eMule, that takes pieces of that file from multiple users in order to speed up the download process.

In sum, Shareaza LE searches for files that are likely to contain child pornography (by file name and hash value), and it narrows the search results to network users in a particular geographic region (by IP address). Once a file of interest is found, Shareaza LE downloads that file from a single user (identified by the user's GUID). That information—the IP address, file name, hash value, and GUID—and the date and time of download are logged. As one of the officers explained, although Shareaza LE "does a little bit more extensive logging than the normal [file-sharing] software," it "doesn't do anything intrusively to get anything." Shareaza LE logs "the information that's presented from establishing that peer-to-peer connection." For example, with respect to the GUID that matches a user's eMule software, that GUID is shared when one user's eMule software exchanges files with another user's eMule software. As for the IP address, one of the officers explained that at least some peer-to-peer software applications display the IP address of the network computers possessing a file available for download.

Here, a forensics analyst for Lane County, Caffee, used Shareaza LE to identify a user with an IP address in

Lane County who was sharing files on the eDonkey network with hash values that matched hash values identified by the NCMEC as child pornography.[5] On October 19, 2011, Caffee downloaded two files from that user. In doing so, Caffee obtained the GUID for the eMule software that was sharing those files. Caffee wrote a report and forwarded it to a detective, Hoberg, who determined that the two files (both videos) depicted sexually explicit conduct involving children.

Using a publicly available website that identifies an ISP based on an IP address,[6] Hoberg determined that Charter Cable controlled the IP address in Lane County that Caffee identified, and he served a grand jury subpoena on Charter Cable to obtain the name and service address of the customer assigned to the IP address. Charter Cable provided the police with a name and physical address, and Hoberg then obtained a search warrant for that address.

When Hoberg executed the warrant, he learned that defendant lived at the address. After Hoberg provided defendant *Miranda* warnings, defendant told him that he "probably" downloaded child pornography using eMule. Defendant further explained that he was trying to obtain adult pornography and tried to avoid any child pornography. He stated that, when using eMule, he selects several videos to download but does not look at individual file names before downloading.

Hoberg seized defendant's computer. When Caffee searched the operable hard drive of that computer, he found eMule software and matched its GUID to the GUID for the two files that Caffee downloaded. Caffee found two other complete video files containing child pornography in the eMule Temp folder on defendant's computer, and he found another child pornography file (an image) in the desktop recycle bin on defendant's computer, which had not been emptied. Caffee also found the search history for defendant's eMule software and identified search terms commonly associated with child pornography.

---

[5] Caffee did not know the particular search terms Shareaza LE used to find those files, but one of the files contained the terms "10Yo" and "Webcam" and the other contained the terms "Incest" and "13yo" and described a sex act.

[6] Several publicly available websites allow a person to input an IP address and find the city, state, and ISP associated with that IP address.

Defendant was charged with two counts of first-degree encouraging child sexual abuse, ORS 163.684, relating to the two video files Caffee downloaded from defendant on the network, and three counts of second-degree encouraging child sexual abuse, ORS 163.686, relating to the other three files found on defendant's computer.[7]

Defendant filed a motion to suppress the evidence obtained by the "warrantless search" of the eDonkey peer-to-peer network (*i.e.*, the IP address and other information obtained by Shareaza LE) and all derivative evidence (defendant's statements to police and evidence obtained as a result of the computer search). Defendant argued that Shareaza LE was equivalent to "surreptitious government surveillance" of his private communications on a peer-to-peer network:

> "Like a phone line, eMule, Gnutella, any of the other file sharing programs allow a form of communication between people, and what the State is saying is that there is no right to privacy in that which may be communicated along that phone line.
>
> "The GUID, the IP address, it's a communication. If a police officer wants to tap someone's phone, they need a warrant. They can't create a global, all-encompassing phone-tap machine and then say, but, we filtered it out, so it only picks out these specific words, so it only picks [terms commonly used to search for child pornography]. They can't do it because it's too much of an invasion of privacy.
>
> "Really, I think the cases here show that it's not always enough to say: (1) that this information is available to third parties; therefore, it's freely available to the police

[7] ORS 163.684 provides, in part, that "[a] person commits the crime of encouraging child sexual abuse in the first degree if the person *** [k]nowingly *** disseminates * * * a visual recording of sexually explicit conduct involving a child" and "[k]nows or is aware of and consciously disregards the fact that creation of the visual recording of sexually explicit conduct involved child abuse."

ORS 163.686 provides, in part, that "[a] person commits the crime of encouraging child sexual abuse in the second degree if the person *** [k]nowingly possesses or controls * * * a visual recording of sexually explicit conduct involving a child for the purpose of arousing or satisfying the sexual desires of the person or another person" and "[k]nows or is aware of and consciously disregards the fact that creation of the visual recording of sexually explicit conduct involved child abuse."

> however they choose to get it; and (2), there's a clear hostility towards this sort of surveillance *** towards 24-hour non-human surveillance without a warrant."

With respect to "non-human surveillance," defendant contrasted an officer's on-the-street surveillance with "invasive" surveillance by "means of technology" that courts had determined to be a "search," *e.g.*, "GPS tracking" and "thermal imaging of homes." Defendant argued that, like those government activities, "the government's current system for gathering information constitutes searching in and of itself" and "simply goes too far."

In response, the state argued that defendant had no privacy interest in the information police obtained using Shareaza LE. That conclusion was warranted, in the state's view, because defendant "made the decision to join a public file-sharing network for the purpose of sharing, in his case, child pornography." And the state asserted that the officer's activity was "just like anybody else's. I could go onto eMule and I could find any number of individuals that were distributing child pornography, just as a user. There [are] no privacy interests there."

After hearing those arguments, the trial court denied defendant's motion:

> "While there are many different permutations and considerations from many different angles, I think at the heart of it is this, [defendant] availed himself of a public networking peer-to-peer computer program that gave him access, knowingly, to countless other people who did the same.
>
> "That act and engaging in this network subjected himself to public viewing and evaluation by anybody who wished to be part of that network, and as such there was no violation of one's right to privacy by having law enforcement do the same."

Defendant later entered a conditional guilty plea for all crimes charged, preserving an appellate challenge to the trial court's denial of his motion to suppress.

On appeal, defendant again argues that the police engaged in a warrantless search under Article I, section 9, when they used Shareaza LE. Defendant contends that,

even though his IP address and activity on the network were exposed to other network users, the officers in this case invaded a protected privacy interest by obtaining that information because "a network user does not need or use that information to download a file" and would "have no reason to expect that another [network] participant will deliberately identify [that user's] IP address." Defendant further argues that Shareaza LE, which he calls "advanced computer technology," represented an invasion of privacy because it allowed the police to conduct "continuous, minute scrutiny of Internet activity, log data regarding that activity into a database that permits them to zero in on a specific computer user in a specific place at a specific time, and investigate and capture the content of an individual computer user's shared files."[8]

The state responds that the police did not conduct a search when they used software to identify and download files from his computer that he had made publicly available to other users of the file-sharing network. Shareaza LE, the state emphasizes, "exposed nothing more than what defendant chose to make public by using the file-sharing network." In the state's view, "the proper inquiry for constitutional purposes is not whether the technology used by police is 'advanced,' but whether the police used technology to observe what would otherwise be unobservable without the technology."[9]

---

[8] Defendant does not challenge the officers' use of a subpoena to his ISP to match his IP address with a customer name and physical address. *See State v. Delp*, 218 Or App 17, 20, 26-27, 178 P3d 259, *rev den*, 345 Or 317 (2008) (concluding that the defendant did not have a protected privacy interest in records independently maintained by his ISP, which contained "the name, address, telephone number, subscriber number, local and long distance telephone billing records, length of service, and types of services utilized" for the defendant's account). And he does not challenge the lawfulness of the warrant to search the computers at that address.

[9] The state also argues that defendant failed to preserve the arguments he makes on appeal. We disagree. As detailed above, defendant argued in the trial court that the officers conducted a search, even if they accessed "information *** available to third parties," and he asserted that "non-human surveillance" like Shareaza LE was so "invasive" that it should be treated like other technology that courts had determined to be a "search," *e.g.*, "GPS tracking" and "thermal imaging of homes." In making those arguments, which track the arguments defendant makes on appeal, defendant provided the trial court with an opportunity to identity its alleged error with enough clarity to permit it to consider and correct the error immediately. *State v. Wyatt*, 331 Or 335, 343, 15 P3d 22 (2000).

The parties' competing arguments reflect familiar Article I, section 9, principles. A "search" under Article I, section 9, occurs when "the government invades a protected privacy interest." *State v. Meredith*, 337 Or 299, 303, 96 P3d 342 (2004). We determine whether the government invaded a person's protected privacy interest "by an objective test of whether the government's conduct 'would significantly impair an individual's interest in freedom from scrutiny, *i.e.*, his privacy.'" *State v. Wacker*, 317 Or 419, 425, 856 P2d 1029 (1993) (quoting *State v. Dixson/Digby*, 307 Or 195, 211, 766 P2d 1015 (1988)). "The threshold question in any Article I, section 9, search analysis is whether the police conduct at issue is sufficiently intrusive to be classified as a search." *Id*. at 426. Here, then, we must determine whether the officers' use of Shareaza LE to seek out and download files from defendant on a peer-to-peer network—and to obtain the IP address, GUID, and hash value associated with those files—invaded defendant's protected privacy interest and was thus "sufficiently intrusive to be classified as a search." *Id*.

Although that question cannot be answered by close factual analogy to our precedents under Article I, section 9,[10] we find two cases particularly instructive in applying

[10] Although the issue has not been considered under Article I, section 9, several federal courts of appeals have considered whether users of peer-to-peer computer networks have a reasonable expectation of privacy, under the Fourth Amendment to the United States Constitution, in files and associated information that they share on the network. Those courts have uniformly held that users do not. *See U.S. v. Borowy*, 595 F3d 1045, 1048 (9th Cir 2010), *cert den*, ___ US ___, 131 S Ct 795 (2010) (concluding that, because the defendant "lacked a reasonable expectation of privacy in the shared files [on a peer-to-peer network], [an agent's] use of a keyword search to locate these files did not violate the Fourth Amendment" and rejecting the argument "that the use of a 'forensic software program' that is unavailable to the general public to confirm that the files contained child pornography rendered [the agent's] conduct an unlawful Fourth Amendment search"); *U.S. v. Ganoe*, 538 F3d 1117, 1127 (9th Cir 2008) ("[W]e fail to see how [an objectively reasonable] expectation [of privacy] can survive [the defendant's] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program."); *U.S. v. Stults*, 575 F3d 834, 843 (8th Cir 2009) ("We hold that [the defendant] had no reasonable expectation of privacy in files that the FBI retrieved from his personal computer where [the defendant] admittedly installed and used [file-sharing software] to make his files accessible to others for file sharing."); *U.S. v. Perrine*, 518 F3d 1196, 1205 (10th Cir 2008) ("[A]s [the defendant] conceded, he had peer-to-peer software on his computer, which permitted anyone else on the internet to access at least certain folders in his computer. To the extent such access could expose his

that provision to an officer's use of software to access files shared on a peer-to-peer network: *State v. Campbell*, 306 Or 157, 759 P2d 1040 (1988), and *Wacker*. Each involved police use of technology to collect or record information about a suspect, and, in each, the Supreme Court considered police observation of conduct that was, at least arguably, observable by others.

In *Campbell*, officers suspected that the defendant was involved in several burglaries, and they attached a transmitter to the defendant's car while it was parked in a public parking lot. 306 Or at 159-60. By tracking radio waves emitted by the transmitter from a small airplane, the officers were able to monitor the movement of the car over the course of several days, and they eventually located the car at a residence that had been burglarized. The Supreme Court concluded that the use of the radio transmitter to locate the defendant's car amounted to a search under Article I, section 9. The court explained that the "use of a radio transmitter to locate an object to which the transmitter is attached cannot be equated with visual tracking"—the police had failed to visually monitor the defendant's car without detection. *Id.* at 171-72. And the court reasoned that "[a]ny device that enables the police to quickly locate a person or object anywhere within a 40-mile radius, day or night, over a period of several days, is a significant limitation on freedom from scrutiny." *Id*. at 172.

In *Wacker*, after receiving complaints from a tavern owner of drug activity in the area, officers used a video camera and starlight scope (a device that magnified images and helped officers see better in the dark) to observe the defendant and others inside a car parked in the tavern

---

subscriber information to outsiders, that additionally vitiates any expectation of privacy he might have in his computer and its contents."); *U.S. v. Conner*, 521 F App'x 493, 498 (6th Cir 2013) (same). *See also, e.g.*, *State v. Roberts*, 2015 UT 24, ¶ 28, 345 P3d 1226, 1236 (Utah 2015) (concluding that use of software not available to the public to access peer-to-peer network was not an unlawful search under the Fourth Amendment); *State v. Peppin*, No. 32058-8-III, WL 1592442 at *6 (Wash App Div 3, Apr 9, 2015) (concluding, under state constitutional provision, that "a person's private affairs are not disturbed when law enforcement uses peer to peer software to view files that the person voluntarily shares with the public on his or her computer").

parking lot. 317 Or at 421. In concluding that the officers had not conducted a search under Article I, section 9, the court observed that the defendant "chose to carry out his activities in the parking lot of a tavern that was open for business" while he was "in a car with its console or overhead light on." *Id*. at 427-28. Although the police observed the defendant at night, his conduct was visible to passersby and to the officers who were stationed 29 feet away. Rejecting the notion that *Campbell* "establish[ed] a *per se* rule against the warrantless use by police of any technologically enhanced observation regardless of the circumstances," *id*. at 426 n 12, the court concluded that the "open-to-the-public nature of defendant's *** location and activities in a lighted car in a tavern parking lot during business hours establishes that no government conduct significantly impaired defendant's privacy," *id*. at 427.

In comparing the police conduct in *Campbell* and *Wacker*, there are two constitutionally significant distinctions that are instructive here. First, the conduct that the police observed in *Wacker* was available to public observers in a way that the information the police gained from the transmitter in *Campbell* was not. In *Wacker*, the officers' use of a starlight scope and camcorder to aid and record their observations did not amount to a search because the officers used those devices to observe conduct that was observable by any passerby in the parking lot. In *Campbell*, though, the court rejected the contention that "the transmitter disclosed only what any member of the public could legitimately have observed." 306 Or at 165. The officers in that case had failed to track the defendant's car through visual surveillance, and it would be impossible for the police or the public to observe the kind of information that the transmitter provided. *See* Wayne R. LaFave, 1 *Search and Seizure* § 2.7(f), 999 (5th ed 2012) (criticizing the notion that a radio transmitter attached to a car traveling on public roads reveals the same information that any member of the public would observe because "[o]nly an army of bystanders, conveniently strung out on [the defendant's] route and who not only 'wanted to look' but also wanted to pass on what they observed to the next in line, would *** 'have sufficed to reveal all of these facts to the

police'").[11] In other words, the conduct that the police observed was only nominally public; the transmitter gave the officers access to information that was materially different than the information the defendant broadcast to those who could see him traveling in his car.

Second, and relatedly, to the extent that *Campbell* and *Wacker* both considered official observation of conduct in a public place, the surveillance in *Campbell* was of a dramatically different scope and intensity than that in *Wacker*. In *Wacker*, the officers' surveillance was targeted to detecting drug activity in a particular tavern parking lot. The court was emphatic that the defendant "chose to carry out his activities" in a lighted car in that public space. 317 Or at 426. By contrast, the transmitter in *Campbell* allowed the police to conduct pervasive surveillance of the defendant: Day and night, over a period of several days, the officers could track the defendant's movements within a 40-mile radius, whether his vehicle was on a busy city street or a secluded highway. 306 Or at 172. Given the breadth of information that the police learned from the transmitter, the court reasoned that, if police could use the transmitter without limitation, "no movement, no location, and no conversation in a public place would in any measure be secure from prying of the government."[12] *Id.*

---

[11] The court in *Campbell* cited an earlier version of the LaFave treatise in support of the notion that monitoring a transmitter on a car could not be equated with visual tracking. *See Campbell*, 306 Or at 172 (citing Wayne R. LaFave, 1 *Search and Seizure* § 2.7(d) (2d ed 1987)).

[12] The Supreme Court has focused on another aspect of the conduct in *Campbell* in distinguishing it from police conduct that the court concluded was not a search. In *State v. Smith*, 327 Or 366, 373 n 5, 963 P2d 642 (1998), in concluding that dog sniffs in public places are not searches, the court noted that *Campbell* "involved a clear form of invasion, a *trespass*. The tracking device at issue was attached without permission to the defendant's privately owned vehicle." (Emphasis in original.)

But the court went on to say that it was not holding that, "to qualify as a search, the invasion always must be of the type that the law traditionally has labeled as a 'trespass'—an actual physical intrusion." *Id.* at 373. The court explained that, "if Article I, section 9, is to have any meaning, it must be read in light of the ever-expanding capacity of individuals and the government to gather information by technological means. It must, in other words, speak to every possible form of invasion—physical, electronic, technological, and the like." *Id.* Thus, although we acknowledge that *Campbell* involved a trespass and this case does not, the absence of a trespass is not dispositive in this case, which involves the use of a computer program to access information on a peer-to-peer network.

In subsequent cases, the Supreme Court has highlighted both the not-truly-public nature of the information that the transmitter in *Campbell* collected and the extensive surveillance that the transmitter allowed. In *Meredith*, where the court concluded that police did not conduct a search when they attached a transmitter to a public employee's publicly owned car, the court explained that

> "[t]he officers [in *Campbell*] subjected the defendant and his vehicle to pervasive and constant examination of his movements and location throughout his daily life. In the same way that electronically eavesdropping on public conversations would enable the police to gain information that, although nominally public, was not normally available to a passerby, the police monitoring of the transmitter allowed the government to observe a range of conduct that normally would have been inaccessible to the general public or to government officials."

337 Or at 306-07 (reasoning that the defendant, as a public employee, "did not have a protected privacy interest in keeping her location and work-related activities concealed from the type of observation by her employer that the transmitter revealed"). In this case, those same considerations compel the conclusion that the officers' conduct—the use of Shareaza LE on a peer-to-peer network—was not sufficiently intrusive to be classified as a search.

First, the officers obtained the same information with Shareaza LE that was available to other network users. When defendant made files available for download on the eDonkey network, defendant made the IP address and GUID associated with those files available to other users. Whereas the transmitter in *Campbell* gave police access to information about the defendant that was "inaccessible to the general public or to government officials"—the location of the defendant's car at any time over a span of several days—here the information that the police observed using Shareaza LE is the same information that any user with file sharing software could access. *Meredith*, 337 Or at 307. And that information was available to the officers, as it was to other users of the network, because defendant chose to share files with those users, just like the defendant

in *Wacker* chose to carry out his activities in a place where others could see it.[13]

Second, the officers used Shareaza LE to seek out files containing child pornography that users were sharing on a peer-to-peer network; that technology did not allow the "pervasive and constant examination of [defendant's online activity] throughout his daily life" as the transmitter in *Campbell* did with respect to the defendant's movements. Indeed, the police conduct here was more like the limited observation of particular conduct that was not a search in *Wacker*. *Meredith*, 337 Or at 307. The officers here used Shareaza LE to target files of child pornography that users made available on the network, and the officers then downloaded two of those files from a particular user (who was later identified as defendant). In doing so, it was not necessary for police to engage in constant, prolonged observation of defendant's conduct on the network.

Defendant responds with two arguments. With respect to the proposition that he had no privacy interest in the information he made available to others on the network, defendant argues that he expected to remain anonymous to other network users, who were simply interested in downloading his files. That is, defendant asserts that, even though he made his IP address and other information available when he shared files, he had "no reason to expect that another participant [would] deliberately identify [his] IP address" or "log [his] activity on the network." We disagree.

The Supreme Court has repeatedly rejected the notion that a person's "subjective expectation of privacy *** necessarily determine[s] whether a privacy interest has been violated." *State v. Brown*, 348 Or 293, 298, 232 P3d 962 (2010). In *State v. Howard/Dawson*, 342 Or 635, 643,

[13] We note that, contrary to defendant's suggestion, the fact that police were engaged in a "determined effort" to find network users who were sharing child pornography cannot be equated with police efforts to create a situation that forced defendant to expose information to others—conduct that has been deemed a search. *See State v. Nagel*, 320 Or 24, 31, 880 P2d 451 (1994) (concluding that an officer conducted a "search" under Article I, section 9, when he conducted a field sobriety test because, in doing so, "[t]he officer created a situation that exposed information about defendant that was otherwise not observable by either the officer or by members of the general public").

157 P3d 1189 (2007), for example, the court concluded that the defendants did not retain a privacy interest in garbage that they turned over to a sanitation company without any restriction on its disposal, even though the defendants "did not expect that the sanitation company would look through their garbage or permit someone else to do so." We applied that same principle in *State v. Carle*, 266 Or App 102, 110, 337 P3d 904 (2014), *rev den*, 356 Or 767 (2015), where we concluded that the sender of a text message did not retain a privacy interest in the digital copy of the text message found on the recipient's phone, even if the sender "did not expect anyone other than [the recipient] to see the text message—or, at the least *** did not expect law enforcement to see the message." So too here: Defendant did not retain a privacy interest in information that he provided to network users when he made files available for download, even if defendant expected that no other user would take notice of that information or find it particularly useful.

Defendant also asserts that Shareaza LE—what he calls "advanced computer technology"—allowed for the kind of pervasive surveillance that the court found was a search in *Campbell*. He contends that Shareaza LE is just like the transmitter used in *Campbell* because it allowed officers to "continuously monitor and scrutinize an immense amount of internet activity both day and night and then track down suspicious activity to a particular geographical location and, ultimately, a single computer." Again, we disagree.

Initially, we take issue with defendant's characterization of Shareaza LE. To say, as defendant does, that Shareaza LE allows for "continuous, minute scrutiny of Internet activity" misapprehends the constraints of Shareaza LE and the way that the police used it here. Because Shareaza LE connects to a peer-to-peer network, its search is limited to files that network users are sharing and to information associated with those files, like an IP address, that is available to other users. In that respect, it operates just like other software that accesses the network. Further, in this case, police used Shareaza LE to conduct targeted scans of shared network files for child pornography.

We are not faced with continuous police monitoring of all of defendant's "Internet activity."[14]

There is no doubt that Shareaza LE creates important efficiencies for the officers in locating a network user sharing child pornography.[15] But the fact that Shareaza LE made police practice more efficient—by allowing for repetition and automation of the procedures an officer would go through without that kind of software—does not by itself establish that police conduct amounted to a search under Article I, section 9. The Supreme Court has "never suggested that use of *any* device or enhancement—no matter where that device or enhancement was used—would qualify" as a "constitutionally significant 'search.'" *State v. Smith*, 327 Or 366, 371, 963 P2d 642 (1998) (emphasis in original); *Wacker*, 317 Or at 426 n 12 (*Campbell* did not establish "a *per se* rule against the warrantless use by police of any technologically enhanced observation regardless of the circumstances"). And the fact that technology has created efficiencies or conveniences in police practice does not mean that police conduct a "search" when they use it. *See Wacker*, 317 Or at

---

[14] Defendant also warns that "the state is not limited in its use of Shareaza LE to finding child pornography; the state could, at any moment, tweak the software to find files expressing political dissent." But those are not the facts before us. On that point, we find helpful the Ninth Circuit's rejection of a similar argument under the Fourth Amendment:

> "Because we decide only the case in front of us, we reject [the defendant's] argument that our decision will allow unrestricted government access to all internet communications. We do not rule on whether, if confronted with different facts—for example, where the information was not already exposed to the public at large, where the hash-mark analysis might reveal more than whether a file is known child pornography, or where the government 'vacuumed' vast quantities of data indiscriminately—we might find a Fourth Amendment violation. Here we are presented only with the limited case of a targeted search of publicly exposed information for known items of contraband."

Borowy, 595 F3d at 1048 n 2.

[15] Instead of an officer manually entering separate search terms associated with child pornography into standard peer-to-peer software, as a network user who wanted to find child pornography would do, Shareaza LE searches the network for several of those terms all at once. The software then filters those search results to identify files (1) with hash values known to be child pornography and (2) with IP addresses thought to be within Lane County. That filtering means that officers do not have to go through "thousands and thousands" of files, one-by-one, to identify files with a hash value predetermined to be child pornography, and they do not have to search "thousands and thousands of different IP addresses" to find a file with an IP address in Lane County.

427 (concluding that use of light-enhancing starlight scope to aid in seeing activity in a car parked in public parking lot was not a search, even though it allowed police to conduct surveillance without detection 29 feet away from car); *State v. Ainsworth*, 310 Or 613, 618, 801 P2d 749 (1990) (concluding that police use of helicopter to view the defendant's property from the air was not a search, and explaining that, "[w]hether on foot, by motor vehicle, boat, tall building, promontory, air balloon, or aircraft—the manner is unimportant if the officers are at a location where they are lawfully entitled to be"); *State v. Louis*, 296 Or 57, 61, 672 P2d 708 (1983) (concluding that there was no search when police used a telephoto lens, which allowed for "modest enlargement," to photograph activities inside of home from other side of street, where activities could be seen from the street without a telephoto lens).

Rather, the controlling questions as to whether police conducted a search, as shown by cases like *Wacker* and *Campbell*, are whether police were able to obtain information that was materially different from information the defendant made available to others and whether the police conduct swept so broadly that it amounted to pervasive surveillance of the defendant's daily life. Here, the answer to both those questions is "no." The information that police obtained using Shareaza LE—particularly the IP address—was the same information that was available to any other user of the network. The police obtained that information by zeroing in on shared files that contained child pornography, not by engaging in all-encompassing surveillance of defendant's online activity. Accordingly, we conclude that the police did not conduct a search under Article I, section 9, and the trial court did not err in denying defendant's motion to suppress.

Affirmed.